

REMARKS

Reconsideration of this application is requested in light of the following remarks. No claims are amended, added or cancelled via this response. Claims 1-20 remain pending in this application.

CLAIM REJECTION UNDER 35 USC § 103

In the Office Action, claims 1-20 are rejected under 35 USC 103(a) as being unpatentable over Vij et al. (US Patent 6,452,910, hereafter Vij) in view of Karaoguz et al. (US Patent 7,114,010, hereinafter Karaoguz). Applicant respectfully traverses the rejection.

Vij discloses a wireless bridge, which provides an end-to-end wireless communication path between a Bluetooth-enabled device (e.g., a Personal Digital Assistant, Internet-enabled cellular phone or vehicle module) and an Internet-connected server (Figures 1 and 6; col. 3, lines 24-28). The wireless bridge includes a wireless LAN interface (wireless LAN I/F, Figure 6) and a Bluetooth interface (Bluetooth I/F, Figure 6). Transmission of data between the wireless bridge and the server is via the wireless LAN interface, and exchange of data between the wireless bridge and a Bluetooth-enabled device is via the Bluetooth interface (col. 6, lines 39-54). A permanent virtual circuit is established via TCP between the wireless bridge and the Internet-connected server to carry all vehicle communications (col. 6, lines 46-48). The wireless bridge reformats incoming data (RS-232 data stream) from the vehicle module and sends it to the server on a TCP/IP network. The server translates the TCP/IP stream to an RS-232 data stream (col. 7, lines 14-22).

Every bridge has a zone, which is defined as the area around it within which Vehicle Modules can set up connections (col. 8, lines 19-21). When a vehicle enters a zone, the bridge establishes a link with the vehicle's Vehicle Module, and advises the server that the link has been established (col. 8, lines 31-37). When a vehicle enters an overlapping zone, the bridge in the new zone will not detect the vehicle, and only when the signal power degrades such that the old connection gets broken does the Vehicle Module set up a connection with the bridge in the

new zone (col. 8, lines 38-43). When a vehicle leaves a zone, the bridge and the Vehicle Module detect signal strength loss and disconnect (col. 8, lines 60-63).

With respect to claim 1, the Office Action is equating the elements of Applicant's claims with features disclosed in Vij as follows:

#	Applicant's Claim Elements	Vij
1	Conducting wireless data communications with mobile units using a first wireless communication protocol	A communication system that provides a wireless link for wireless communications with a Bluetooth enabled vehicle (Fig. 6, col. 6, lines 39-44)
2	Network interface of the access point	Wireless bridge (Fig. 6)
3	Host computer	Data Acquisition System (Fig. 6)
4	Cable connection	Vehicle data is obtained by the wireless bridge from the Data Acquisition System via the Bluetooth link (col. 6, lines 48-50)

Applicant believes that certain of the characterizations of Vij, which are made in the Office Action, are fundamentally incorrect. In particular, the Office Action states that Vij discloses "receiving, by a network interface of the access point, the management communications from the host computer over a cable connection." Applicant respectfully disagrees. Referring to item 2 of the above comparative chart, the Office Action equates the "network interface of the access point" with the Wireless Bridge of Vij. Referring to item 3 of the above comparative chart, the Office Action also equates the "host computer" with the Data Acquisition System of Vij. As Fig. 6 of Vij and the supporting description clearly indicate, the Wireless Bridge and the Data Acquisition System communicate over a wireless, Bluetooth link (see the link between the "Bluetooth I/F" and the "Bluetooth enabled Vehicle Module", Fig. 6).

Accordingly, Vij does not disclose a network interface of an access point receiving management communications from a host computer over a cable connection (or a hardwired network interface, as is claimed in claim 12). In Vij, the Wireless Bridge and the Data Acquisition System (via the Bluetooth enabled Vehicle module) communicate over a wireless link, and not over a cable connection.

The Office Action (on page 3) goes further to state that Vij does not expressly disclose: “when a communication failure between the host computer and the access point occurs over the cable connection, a radio module of the access point receiving the management communications from a wireless terminal that is distinct from the host computer over a wireless connection using a second wireless communications protocol to allow management of the access point, wherein the second wireless communication protocol is different from the first wireless communication protocol.” Applicant agrees that Vij does not disclose the above feature of Applicant’s claims.

However, the Office Action asserts that the above feature of Applicant’s claims is disclosed by Karaoguz. Applicant respectfully disagrees.

Karaoguz discloses techniques for controlling and managing network access that are used to enable a wireless communication device to selectively communicate with several wireless networks (Abstract). A multi-mode communication device 30, 34 (FIG. 1) may communicate with one or more wireless communication devices 26, 28, 32 (FIG. 1; col. 4, lines 15-18). Embodiments of multi-mode communication devices may include multiple processing networks 42-44 that are coupled to a single radio interface 46 and antenna 48 (FIG. 2) or multiple network processors 60-62 that are coupled to multiple radio interfaces 68-70 and antennas 72-74 (FIG. 3) (FIG. 2 and 3; col. 4, line 39 through col. 5, line 25). In the former embodiment, a multi-mode controller 40 (FIG. 2) manages network access to two or more wireless networks (col. 4, lines 41-43). In the latter embodiment, a network selector 64 routes signals from one component to another (col. 5, lines 7-9). Dual mode operation is achieved by a dual mode controller (DMC) (col. 6, lines 14-17). In an embodiment, a dual-mode mobile communication device is capable of accessing either a Bluetooth or a Point-Controller (PC) controlled IEEE 802.11b network

(FIG. 11; col. 10, lines 5-11). In such an embodiment, the DMC initiates a network scan to search for an 802.11b PC beacon (block 236, FIG. 14) and, when the PC beacon is received, the device may join the 802.11b network (FIG. 14; col. 11, lines 22-34). If the user does not approve connecting to the 802.11b network or if the initial 802.11b network scan fails to find a PC beacon, the DMC starts a Bluetooth inquiry scan (block 248, FIG. 14) to search for the existence of a Bluetooth network 248 (FIG. 14; col. 11, lines 47-53). If the unit receives a valid inquiry code (block 250, FIG. 14), a connection setup procedure is performed (block 254, FIG. 14) (col. 11, lines 64-67).

As mentioned above, Applicant respectfully disagrees that Karaoguz discloses the claimed feature of: “when a communication failure between the host computer and the access point occurs over the cable connection, a radio module of the access point receiving the management communications from a wireless terminal that is distinct from the host computer over a wireless connection using a second wireless communications protocol to allow management of the access point, wherein the second wireless communication protocol is different from the first wireless communication protocol.”

First of all, nowhere does Karaoguz disclose “a cable connection” (or a hardwired network interface, as is claimed in claim 12) between an access point and a host computer. The wireless communication device of Karaoguz is disclosed only to communicate over wireless links (see Karaoguz, FIG. 1). Additionally, nowhere does Karaoguz disclose the concept of “a communication failure between a host computer and an access point occurring over a cable connection”. In contrast, Karaoguz discloses search procedures carried out by a dual mode controller (DMC) of a multi-mode communication device for the purpose of establishing communications with an 802.11b or Bluetooth network (see Karaoguz FIG. 14 and col. 11, lines 22-67). Nowhere is the concept of a communication failure between a host computer and an access point over a cable connection disclosed by Karaoguz. Additionally, nowhere does Karaoguz disclose an access point “receiving management communications . . . to allow management of the access point.” Instead, Karaoguz only discloses switching between networks to provide high speed Internet access, voice services, data services, and multimedia services (see

Karaoguz, Abstract). For at least the above reasons, Applicant contends that Karaoguz does not disclose the features of Applicant's claims that the Office Action asserts that Karaoguz discloses.

Neither Vij, Karaoguz nor their combination discloses an access point receiving management communications from a host computer over a cable connection (or a hardwired network interface, as is claimed in claim 12), among other significant features of Applicant's claims 1-20. Based on the above remarks, Applicant believes that the rejection of claims 1-20 under 35 U.S.C. 103(a) has been overcome. Accordingly, Applicant respectfully requests that this rejection be reconsidered and withdrawn, and that claims 1-20 be allowed.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending are in condition for allowance. A Notice of Allowance is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (480) 385-5060 or sschumm@ifllaw.com.

If necessary, the Commissioner is hereby authorized to charge payment or credit any overpayment to Deposit Account No. 50-2091 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly extension of time fees.

Respectfully submitted,
Ingrassia Fisher & Lorenz, P.C.

Date March 5, 2009

By /SHERRY W. SCHUMM/
Sherry W. Schumm
Reg. No. 39,422
(480) 385-5060